INSTITUTE FOR DEFENSE ANALYSES

Enterprise Considerations for Ports and Protocols

William R. Simpson

Kevin E. Foltz

October 21, 2016

IDA Non-Standard
NS D-8011
Log: H 2016-000647
Copy

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task BC-5-2283, "Architecture, Design of Services for Air Force Wide Distributed Systems," for USAF HQ USAF SAF/CIO A6. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Enterprise Considerations for Ports and Protocols

Kevin Foltz and William R Simpson

***Abstract*—The need to control information flow to a restricted set of accepted protocols arises from the vulnerabilities that may come from any protocol. Reducing the acceptable protocols to a small set of well-tested standard protocols will reduce the attack surface and provide high confidence in selected communications. These protocols are restricted to specific ports or addresses in the receiving web service. HTTPS is familiarly restricted to port 443. In the standard nomenclature, this traffic may be configured as either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). The standard ports are defined by Internet Assigned Numbers Authority (IANA). The IANA is responsible for maintaining the official assignments of port numbers for specific uses. However, many unofficial uses of both well-known and registered port numbers occur in practice. Screening of acceptable ports and protocols has been done, in the past, by network appliances known as firewalls. Communications on the approved list were permitted, others blocked. However, many appliances now have such functionality and the server or service may have a host-based security system that can apply this functionality. This paper covers enterprise considerations for screening of ports and protocols.**

***Index Terms* — Appliance, Firewall, IT Security, Traffic Inspection.**

I. INTRODUCTION

Guidance and policies that govern the use, configuration, and management of the communication protocols in use by the web services and applications that are connected to the network are required for interoperability and security. Policies specify the proper use of Port, Protocols, and Services (PPS) in order to control what types of communications are allowed to cross the boundaries of the networks. Basically, a port is an access channel to and from a specific service, and a protocol is a standardized way for computers to exchange information. Data on the network is sent and received by software that automatically organizes such data to be transferred into packets, made in a standardized way (defined by the protocol in use) so that the destination host can recognize them as data and properly decode them. Network clients use different ports or channels (which are given standardized numbers) to transfer data. The port number (and the destination IP address) is included as part of the header each packet is given in order to deliver the packet to the proper end-point service. The policies on PPS are typically enforced by network and security appliances and software such as routers, firewalls, and intrusion detection/protection devices that protect the boundary of the network or reside at the end-points (i.e., web services or clients).

Manuscript received June 1, 2016; revised July 30, 2016. This work was supported in part by the U.S. Secretary of the Air Force and The Institute for Defense Analyses (IDA). The publication of this paper does not indicate endorsement by any organization in the Department of Defense or IDA, nor should the contents be construed as reflecting the official position of these organizations

K. Foltz is with the Institute for Defense Analyses. (email: kfoltz@ida.org)
William R. Simpson is with the Institute for Defense Analyses, 4850 Mark Center Drive, Alexandria, Virginia 22311 USA and is the corresponding author phone: 703-845-6637, FAX: 703-845-6848 (e-mail: rsimpson@ida.org)

Originally, the transmission was done at half duplex, and two ports were needed for the control program. Eventually, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) were adopted, and only one port was needed. TCP and UDP port numbers are also used by other protocols. The Internet Assigned Numbers Authority (IANA) maintains the official assignments of port numbers for specific uses [1]. However, many unofficial uses of both well-known and registered port numbers occur in practice. A few ports and their usage are given in Table 1. There are 65,535 ports available as a 16-bit unsigned integer.

Table 1 Some Example Ports and Protocols

Port	Protocol	Messaging Protocol	Status
18	TCP, UDP	The **Message Send Protocol** (MSP) is an application layer protocol. Defined in RFC 1312 [2].	Official
80	TCP, UDP	**Hypertext Transfer Protocol (HTTP).** RFC 2068 [3]	Official
110	TCP	**Post Office Protocol v3 (POP3)** is an email retrieval protocol. RFC 1081 [4]	Official
143	TCP	**Internet Message Access Protocol (IMAP)** e-mail retrieval and storage as an alternative to POP. Defined in RFC 3501 [5]	Official
161	UDP	**Simple Network Management Protocol (SNMP)** defined in RFC 3411[6].	Official
213	TCP, UDP	**Internetwork Packet Exchange (IPX)** RFC 1132 [7]	Official
443	TCP, UDP	**Hypertext Transfer Protocol over TLS/SSL (HTTPS)** RFC 2818. [8]	Official
587	TCP	**Simple Mail Transfer Protocol (SMTP),** as specified in RFC 6409 [9]	Official
1935	TCP	**Adobe Systems Macromedia Flash** Real Time Messaging Protocol (RTMP) "plain" protocol[1]	Official
2195	TCP	**Apple Push Notification** service link[2]	Unofficial
4502	TCP, UDP	**Microsoft Silverlight connectable ports under non-elevated trust** [12]	Official
5672	TCP	**Advanced Message Queuing Protocol (AMQP)** ISO/IEC 19464 [13]	Official
8080	TCP	**HTTP alternate**	Official
49342	TCP	**Avanset Exam Simulator (Visual CertExam file format (VCE) Player)[3]**	Unofficial

Ports may be well-known, registered, and dynamic/private:

- Well-Known: Port numbers 0 through 1023 are used for common, well-known services.
- Registered: Port numbers 1024 through 49151 are the registered ports used for IANA-registered services.
- Dynamic/Private: Ports 49152 through 65535 are dynamic ports that are not officially designated for any specific service, and may be used for any purpose. They also are used as ephemeral ports, from which software running on the host may randomly choose a port in order to define itself. In effect, they are used as temporary ports, primarily by clients when communicating with servers. Dynamic/private ports

[1] Adobe proprietary, H. Parmar, M. Thornburgh (eds.) Adobe's Real Time Messaging Protocol, Adobe, December 21, 2012. [10]

[2] Apple proprietary. https://en.wikipedia.org/wiki/Apple_Push_Notification_Service. [11]

[3] Avanset proprietary. http://www.avanset.com/purchase/vce-exam-simulator.html [14]

can also be used by end-user applications, but are less commonly used so. Dynamic/private ports do not contain any meaning outside of any particular TCP connection.

Protocol standards may be:

- Proprietary – Set by an individual developer for use with his products or products developed by members in his consortium. This creates serious interoperability problems among different developers, and is a barrier to entry to new developers who do not agree to consortium rules.
- De Facto – Openly published by an individual developer, but adopted by enough developers that the protocols are widely in use. This promotes interoperability and the open publication removes barriers to entry.
- Standards-body-based – Are industry-wide protocol definitions that are not tied to a particular manufacturer. With standard protocols, you can mix and match equipment from different vendors. As long as the equipment implements the standard protocols, it should be able to coexist on the same network.

Many organizations are involved in setting standards for networking. The most important organizations for the web are:

- International Organization for Standardization (ISO) – A federation of more than 100 standards organizations from throughout the world.
- Internet Engineering Task Force (IETF) – The organization responsible for the protocols that drive the Internet. These standards are cited by reference to their Request For Comment (RFC).
- World Wide Web Consortium (W3C) – An international organization that handles the development of standards for the World Wide Web.

II. COMMUNICATION MODELS

The **Internet Model** is a group of communications protocols used for the Internet and similar networks. The Internet model is commonly known as TCP/IP, because of its most important protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP). TCP/IP provides connectivity specifying how data should be formatted, addressed, transmitted, routed, and received at the destination. This functionality has been organized into four abstraction layers:

- ***Application Layer* –** Example Protocols: **BGP[4], DNS[5], FTP[6], others...**
- ***Transport Layer* –** Example Protocols: **TCP, UDP, DCCP[7], others...**
- ***Internet Layer* –** Example Internet Layer Protocols: **IP[8], ECN[9], IPsec[10], others...**
- ***Link Layer* –** Example Link Layer Protocols: **Ethernet[11], DSL[12], PPP[13], others....**

These layers are used to sort all related protocols according to the scope of the networking involved. IETF documents RFC 1122 [25] and RFC 1123 [26] describe the Internet Protocol suite and model.

An alternative model, the **Open Systems Interconnection (OSI) model** [27], is often used to describe protocols. The OSI model defines protocols in seven layers. The layers are: (1) Physical, (2) Data Link, (3) Network, (4) Transport, (5) Session, (6) Presentation, and (7) Application. The OSI model defines protocol implementations for its layers, and some of the specific details at each layer differ from those of the Internet model.

The OSI model, while popularly referenced, has succumbed to the Internet model. Unless specified, the Internet model will be used in this document.

III. PORTS IN TRANSPORT PROTOCOLS

Two primary transport protocols are used in the Internet, along with a plethora of special purpose ones. In this description, we limit the discussion to TCP and UDP.

For both of these protocols the port information is explicit in the header information, and it can be used by firewalls and servers to make an "accept or drop" decision.

A. *The Transmission Control Protocol*

TCP is one of the core protocols of the Internet Protocol suite and is so common that the entire suite is often called TCP/IP. Residing at the transport layer, TCP provides end-to-end, reliable, ordered, and error-checked delivery of a stream of octets between programs running on computers connected to a local area network, an intranet, or the public Internet. Web browsers use TCP when they connect to servers on the World Wide Web, and it is used to deliver email and transfer files from one location to another. A variety of other higher-layer protocols use TCP/IP, such as HTTP, HTTPS, SMTP, POP3, IMAP, FTP, and their messages are typically encapsulated in TCP packets. TCP also provides a form of message flow control that will adapt its transmission rate to the congestion on the network. Applications that do not require the reliability of a TCP connection may instead use the connectionless User Datagram Protocol (UDP), which emphasizes low-overhead operation and reduced latency rather than error-checking and delivery validation.

TCP uses TCP Port Numbers to identify sending and receiving application end-points on the hosts. Each side of a TCP connection has an associated internet socket, defined as the host IP address and port number reserved by the sending or receiving application. Port 0 is generally reserved and should not be used. Arriving TCP data packets are identified as belonging to a specific TCP connection by its two sockets, that is, the four-tuple from the combination of source host IP address, source port, destination host IP address, and destination port. This means that a server computer can provide several clients with services

[4] Border Gateway Protocol (BGP) I – routing protocol used to route traffic across the Internet. RFC4271.[15]

[5] Domain Name System (DNS) – naming system for any resource connected to the Internet. RFC 1035. [16]

[6] File Transfer Protocol (FTP) – standard network protocol used to transfer computer files over a TCP-based network. RFC 959. [17]

[7] Datagram Congestion Control Protocol (DCCP) – transport protocol that provides bidirectional unicast connections of congestion-controlled unreliable datagrams. RFC 4340. [18]

[8] Internet Protocol (IP) – the principal communications protocol in the Internet protocol suite. RFC 791. [19]

[9] Explicit Congestion Notification (ECN) – an extension to the Internet Protocol. RFC 3540. [20]

[10] Internet Protocol Security (IPsec) – a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. RFC 4945. [21]

[11] Ethernet – a family of computer networking technologies for local area networks. IEEE 802.3. [22]

[12] Digital subscriber line (DSL) – a family of technologies that are used to transmit digital data over telephone lines. DSL. [23]

[13] Point-to-Point Protocol (PPP) – used to establish a direct connection between two nodes. RFC 2516. [24]

simultaneously, as long as the four-tuples differ. A single client can have concurrent requests for a service, as long as the client takes care of initiating any connections to one destination port from different source ports. Well-known applications, running as servers and passively listening for connections typically use TCP ports. Some examples include:

- **FTP (Ports 20 and 21),**
- **SMTP (Port 25),**
- **SSL/TLS, HTTPS(Port 443),**
- **HTTP (Port 80).**

B. *The User Datagram Protocol*

UDP is one of the core members of the Internet protocol suite (the set of network protocols used for the Internet). With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet protocol network without prior communications to set up special transmission channels or data paths. UDP uses a simple transmission model with a minimum of protocol mechanisms and overhead. It has no handshaking dialogues, and thus exposes any unreliability of the underlying network protocol to the user's program. Because this is normally IP over unreliable media, there is no guarantee of delivery, ordering, or duplicate protection. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram. UDP is suitable for purposes for which error-checking and correction either are not necessary or are performed in the application, avoiding the overhead of such processing at the network interface level. Time-sensitive applications often use UDP because dropping packets is preferable to waiting for delayed packets, which may not be an option in a real-time system. If error-correction facilities are needed at the network interface level, an application would use the TCP or Stream Control Transmission Protocol (SCTP), which are designed for this purpose.

UDP uses UDP Port Numbers to identify sending and receiving application end-points on a host, or Internet sockets. Each side of a UDP connection may have an associated port number reserved by the sending or receiving application. However, unlike TCP, a source port is not required for UDP data packets. Packets are identified as belonging to a specific UDP connection by its combination of source host address, source port (if given), destination host address, and destination port.

Some UDP port numbers include:

- **FTP (Port 20),**
- **Encrypted SMTP (Port 26),**
- **and NTP (Port 123).**

IV. THREATS CONSIDERED

Many of the common protocols and services in use have known vulnerabilities and exploits. They must either be prevented from operating or be allowed with mitigations implemented elsewhere. For example, FTP is known to have severe vulnerabilities and should not be used without mitigating actions. Some protocols are so vulnerable and dangerous that they provide unfettered entry to systems in some cases. Threats, once set up in a system, will use unused ports to call out to their control programs. Restrictions should be applied to both incoming and outgoing messaging. In general, the Enterprise Level Security (ELS) should have a "deny all–permit by exception" policy to block all incoming and outgoing ports unless explicitly permitted. Incoming ports are typically controlled, but outgoing ports are sometime left uncontrolled. If some ports are not explicitly blocked for both incoming and outgoing traffic, it may be possible for malicious code to enter through a permitted port of an allowed service, and then to try to open or access other unused ports for malicious purposes, exfiltration of data, or reconnaissance.

Once all acceptable PPSs have been defined for an enterprise, it is necessary to correctly configure the security devices to allow only the permitted PPSs to pass through the enterprise network and to block all others. Constant monitoring of the networks and devices is required to ensure that only the approved PPSs are allowed and that configurations have not been incorrectly modified, either by accident or by malicious intent. Since the collection of permissible PPSs and their mitigations are likely to evolve over time, this is a constant issue.

V. SERVER CONFIGURATIONS

Most servers come with default ports and protocols that include most of the services available to their broad class of users. For example, the IBM WebSphere would default to all of the common ports plus the IBM ports and protocols for all of their services, and perhaps Oracle, etc. In the enterprise, it is not sufficient to use only the defaults provided by the vendors, because these may include banned services or may not include recommended mitigations.

VI. FIREWALLS AND PORT BLOCKING

The network boundary protection devices, such as routers, firewalls, and intrusion detection/protection devices need to be configured to block all message traffic unless it is to or from permitted services on specific ports using permitted protocols.

We consider two primary types of implementation of boundary protection: network firewall devices embedded in the network and endpoint protection functions embedded in the web servers.

A. *Network Firewalls*

Network firewalls can be divided into conventional network firewalls and next-generation network firewalls. Conventional firewalls effectively control access to and from a requested service through PPS filtering. The firewall examines an incoming/outgoing packet's header for the source IP address, source port, destination IP address, destination port, and other parameters available in the packet header, then applies rules to determine which packets are allowed to pass and blocks all others. A stateful firewall is a conventional firewall that also tracks connections by the socket pairs (source IP, source port, destination IP, destination port) and uses the port number of the source IP address to protect against the use of any other egress ports to exfiltrate data. Next-generation firewalls use additional information about the applications or further inspection of the message contents to protect against other forms of attack not detectable by looking at only the packet header. Both types of firewalls perform the basic handling of Ports and Protocol Services (PPS) filtering. Network firewalls protect the perimeter or boundary of a portion of the network using packet header filtering. The primary

concern with network firewalls is to properly configure them to block all protocols except for the ones approved and needed for the services on the trusted side (server side) of the firewall. In addition, it is imperative to make sure the configuration is current with respect to the changing PPS needs and the recommendations and banned services. In addition, the firewall appliance itself must be maintained in a secure condition with current updates and bug fixes.

A network firewall can operate in transparent (or passive) mode with respect to the end-to-end communication between a service requestor and the end-service if it does not break the end-to-end encryption. In transparent mode, the firewall is not able to decrypt the contents of an encrypted packet; it is able to filter only packets based on the packet header information that is in clear text. The alternative is a proxy firewall that breaks the end-to-end connection and operates as a man-in-the-middle. The proxy looks like the service endpoint to the requestor and is able to decrypt the incoming packets and encrypt the outgoing packets. This permits the firewall to perform content filtering on the decrypted packets.

Firewalls (and other security appliances) can be operated in inline filter mode or in observer mode (also known as promiscuous mode). An inline filter resides in the communication path and examines all packets in real time as they traverse the firewall before passing further into the network. An observer firewall is not in the direct communication path and examines a copy of the packet as it transits the firewall. The advantage of inline firewalls is that they can immediately block the first packet of a recognized attack, whereas in observer mode, the first (or first several) packet(s) will be passed to the destination before it can be blocked and damage prevented. The advantages of observer mode include real-time requirements being relaxed so that if the firewall goes down, communication is not halted.

The firewalls should block access to and from all ports that are accessible behind the firewall (on the trusted side) except those that are explicitly permitted. This is called "deny all by default, permit by exception." For example, a rule for the firewall may be added to explicitly permit messages to and from a web server using HTTP on port 80 (e.g., 123.345.567.789:80). Firewalls that cover larger portions of the network or that front many subnets and host computers must be configured to allow any PPS needed by any of the hosts on its trusted side.

Many firewall best-practices documents include details on firewall configurations. (e.g., Cisco Firewall Best Practices Guide or the Defense Information Systems Agency (DISA) Network Infrastructure Technology Review). For example, tunnels require special considerations to make sure packets embedded in the tunnels do not bypass the firewall. The functionality of a network firewall can be implemented as a separate security appliance that resides either in front of the application servers or in the endpoint hosts. In the latter case, each server would implement a packet header filter to perform PPS filtering in its message handling process.

B. *Application Firewalls*

Application Firewalls (AFWs) or application filters are designed to address the specific attacks on web applications and web services, which are not well addressed by other protection devices. AFWs that front applications can be more specific to the particular needs of the application and protect against attacks targeted at the application layer. For example, an AFW could be used to protect email, both incoming and outgoing, to filter for damaging content or specific attachment types. Other types of application filters can examine the signatures on scripts (e.g., Java applets, JavaScript, ActiveX controls), the file extensions, virus scanning, blocking specific content, or use of specific commands.

In general, there are several different choices for deployment of AFWs: (1) as a separate hardware or software security appliance in front of the application, (2) as part of another security device such as a network firewall or content distribution controller, (3) as a cloud service, or (4) as an agent on the Application Server.

The current trend is for security appliances to integrate several functions in a single device to reduce operating costs and physical space requirements. The network firewall, intrusion detection/prevention, and application content filtering are being combined as integrated security appliances. While there are important benefits to this integration, the compromise of such a device could incapacitate all the protection functions at once.

VII. NETWORK FIREWALLS IN ELS

In ELS a network firewall operates in transparent mode, does not decrypt the packets, and is restricted to examining only the packet header. We note this is more restrictive than the capabilities being offered on many newer firewalls that offer more functionality but require the ability to decrypt the packet to examine its content. These types of security appliances will be covered in other documents. In ELS, network firewalls cannot operate as proxy firewalls or perform deep packet inspection since Transport Layer Security[14] (TLS) with mutual authentication between requestor and service is a basic ELS requirement. In Figure 1, a network firewall positioned in front of several servers is shown to illustrate the use of such devices for PPS filtering. The stateful firewall is shown protecting two web services implemented in two separate web servers with IP addresses IP1 and IP2. The firewall is configured to allow only requests to (IP address:port) combinations {e.g., (IP1:443) and (IP2:443)} and responses from them back to the requestor. In this figure, additional security functions such as intrusion protection and application content filtering are not shown, but an implementation of these functions is described in the next section.

A service request message from a service requestor in the form of HTTPS packets, is allowed to pass the firewall only if the destination fields of the packet header are for one of the web servers IP1:443, or IP2:443 and the protocol is HTTPS over TCP. The firewall is not able to decrypt the packets but passes them through the firewall and routes them to the destination server for the establishment of a TLS connection with mutual authentication. If a TLS session is successfully established, then the packets are received, decrypted, and formed into the request message, which is further processed to determine authorization. The authorization material (e.g., SAML token) enclosed in the request message is validated and checked to determine whether the requestor has access rights for the service according to the Access Control procedures. If proper access rights are determined, then the decrypted request

[14] IETF RFC 5246: The Transport Layer Security (TLS) Protocol, Version 1.2, August, 2008. [28]

message and associated access control material are provided to the application/web service. Responses from the application are encrypted by the server and sent through the TLS connection back to the requestor. The response message is routed through the firewall, which is configured to allow responses from the service port back to the requestor. Again, the firewall is in transparent mode and not able to decrypt the packet and acts as a passive element.

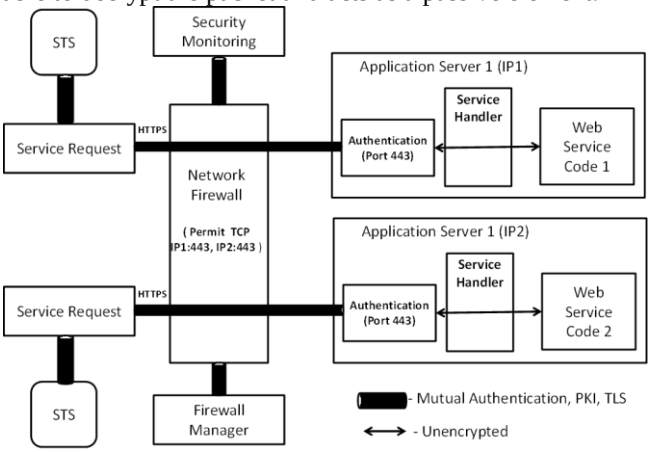

Figure 1 Network Firewall in Transparent Mode

If the web service requires access to services on other ports, then that communication must be routed through a firewall and this must be configured to permit packets on those ports. The firewall may also be considered to be an active element if there is a management interface through which a Firewall Manager can communicate with the firewall for configuration and update activities. This interface requires TLS Mutual Authentication to ensure that only vetted managers are permitted access rights to the firewall.

VIII. ENDPOINT PROTECTION IN ELS

In ELS, an agent-type model is preferred, one in which the packet header filtering and other security functions reside at the web server in the handler chain of the web service. The basic configuration of endpoint protection in ELS, shown in Figure 2, provides a complete set of security functions for packet, message, and application layer security, tailored for the specific web service being protected. Endpoint protection is embedded in the standard ELS web service implementation. The new functions that are added in the Server are Packet Header Inspection, Packet Content Inspection, Message Content Inspection, and Application Protection. These functions implement the PPS protection, as well as other security functions normally provided by network devices such as intrusion detection/protection, packet and message content filtering, deep packet inspection, and application/web content filtering such as that included in an application firewall.

A service requestor establishes communication with the server hosting the target web service according to the ELS practice using HTTPS. The packet is received by the destination sever and the packet header is immediately inspected to perform the PPS blocking, source whitelist/ blacklist checking, and other filtering based on only the header, including stateful tracking of client addresses and ports. Until an HTTPS session has been established, only packets addressed to the server's IP address and port 443 are allowed. Other ports may be opened as needed as part of the web service following HTTPS establishment. Following packet header inspection, the packet is decrypted (if required) and the packet contents are inspected. (Note that prior to establishing a successful HTTPS session, the HTTPS handshake packets are not encrypted and are inspected as delivered). The packet inspection determines whether the packets have unexpected data or other recognized malware or attacks, and if discovered, discards the packet. The accepted packets are then queued and formed into messages. If the server is in the process of establishing an HTTPS session, the messages are delivered to the authentication module to validate the requestor certificates and proceed with HTTPS establishment. Once authenticated, the decrypted messages are delivered to the specific handler of the requested service. The message contents are then inspected for any malformed messages or known attacks. If the message is part of an ELS web service invocation, then the message is processed by the validation models to determine authorization for the service (SAML and XML validation). Following authorization, the sequence of messages is examined to determine whether there is an application-level attack pattern or other anomalies. Following the application protection module, the actions are logged and the message contents and other privileges material are passed to the web service for processing. If any of the modules discovers an issue with the packet, message, or application, then the session is terminated and the security event information is logged.

On the return path, the messages follow a similar process. Messages from the web service are passed to the service handler and examined by the application protection module and then to the message content inspection modules for any suspicious activities and are then handed to the server manager. The server manager modules divide the messages into packets, which are inspected for valid content prior to their encryption. The packet header inspection module will examine the packet to enforce the packet egress rules (only valid egress and destination ports). In effect, the Packet Header Inspection module can perform the required network-layer filtering and can block traffic based on PPS (protocol, IP address, and port).

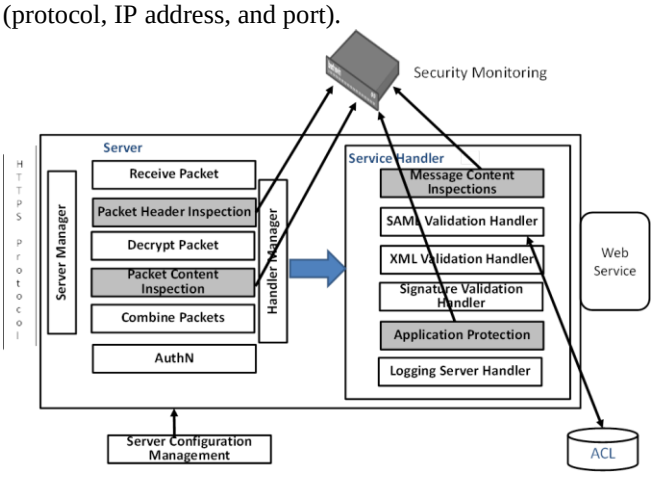

Figure 2 ELS Endpoint Security Functions

In the ELS endpoint protection architecture, the endpoint protection modules can be configured to communicate with additional security monitoring appliances, such as a NetScout[15], that can compile and track statistics about the

[15] Netscout Systems, a network appliance for monitoring net traffic flow, accessed 9/1/2015. https://en.wikipedia.org/wiki/NetScout_Systems [29]

security status of the server and the web service. The security appliances should be active entities and communicate with the server via TLS with mutual authentication. If required, the server could send the decrypted message traffic to other security appliances through this interface for additional security functions, although they would operate in observer mode.

The endpoint protection functions are configured through the server configuration management interface, which communicates with the server by TLS with mutual authentication. The PPS and whitelist information and any software updates are provided through this interface.

It is recommended that the initial configuration of the packet header deny all ports and protocols, both incoming and outgoing, and that permissions be configured in as they are identified as needed, for example HTTPS. If any of the required PPSs violate the forbidden or obsolete list maintained by DISA, then a waiver must be sought.

IX. ADDITIONAL SECURITY HARDENING CONSIDERATIONS

Servers should be hardened by the application of available Security Technical Guidance (STG) documents, where available, or at least the security guides of the server software developer, but these are often insufficient. Server software products have been developed to be resilient, and fault tolerant. Since malicious software is assumed to be present, a request for service may come from within the enterprise bypassing firewalls, and not stating forbidden port numbers. To prevent the server software from finding a protocol resolution software set and assigning the port, all such software should be removed or not installed to begin with. The server software may come with a variety of software subsystems to satisfy a variety of customer needs such as Telnet, secure shell, etc. If the allowable ports are known, the server software installation should not install other software if the installation procedure permits this. If the installation procedure does not allow this, or if the allowable ports and protocols are not worked out until after server software is installed, these non-allowable protocol software sets should be actively sought out and removed.

X. SUMMARY

We have reviewed the ports and protocols used in the Internet model. We have also described the issues they raise and the vulnerabilities that may be introduced. For enterprise operations, having fewer ports open means a reduced attack space. We have also reviewed the specific requirements for an enterprise level security that is bi-laterally authenticated and encrypted end-to-end. This work is part of a body of work for high-assurance enterprise computing using web services. Elements of this work are described in [30-33].

REFERENCES

[1] Michelle Cotton; Lars Eggert et al. (August 2011). Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry. IETF. BCP 165. RFC 6335. http://tools.ietf.org/html/rfc6335

[2] RFC 1312 Message Send Protocol 2 April 1992. http://tools.ietf.org/html/rfc1312

[3] RFC 2068 Hypertext Transfer Protocol HTTP/1.1. January 1997. http://tools.ietf.org/html/rfc2068

[4] RFC 1081 Post Office Protocol – Version 3 November 1988. http://tools.ietf.org/html/rfc1081

[5] RFC 3501 Internet Message Access Protocol – Version 4 rev1 March 2003. http://tools.ietf.org/html/rfc3501

[6] RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, Dec 2002. http://tools.ietf.org/html/rfc3411

[7] RFC 1132 A Standard for the Transmission of 802.2 Packets over IPX Networks, November 1989. http://tools.ietf.org/html/rfc1132

[8] RFC 2818 HTTP Over TLS May 2000. http://tools.ietf.org/html/rfc2818

[9] RFC 6409 Message Submission for Mail November 2011. http://tools.ietf.org/html/rfc6409

[10] Adobe proprietary, H. Parmar, M. Thornburgh (eds.) Adobe's Real Time Messaging Protocol, Adobe, December 21, 2012. http://www.adobe.com/content/dam/Adobe/en/devnet/rtmp/pdf/rtmp_specification_1.0.pdf

[11] Apple proprietary. https://en.wikipedia.org/wiki/Apple_Push_Notification_Service.

[12] Microsoft Siverlight, accessed 1 Sept 2015. https://en.wikipedia.org/wiki/Microsoft_Silverlight

[13] ISO/IEC 19464:2014, Information technology – Advanced Message Queuing Protocol (AMQP) v1.0 specification. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=64955

[14] Avanset proprietary. http://www.avanset.com/purchase/vce-exam-simulator.html

[15] RFC4271Border Gateway Protocol 4 (BGP-4), January 2006. http://tools.ietf.org/html/rfc4271

[16] RFC 1035 Domain Names – Implementation and Specification, November 1987. http://tools.ietf.org/html/rfc1035

[17] RFC 959 File Transfer Protocol (FTP), October 1985. http://tools.ietf.org/html/rfc959

[18] RFC 4340 Datagram Congestion Control Protocol (DCCP) – March 2006. http://tools.ietf.org/html/rfc4340

[19] RFC 791Internet Protocol (IP) September 1981. http://tools.ietf.org/html/rfc791

[20] RFC 3540. Explicit Congestion Notification (ECN) - an extension to the Internet Protocol. [20] Robust Explicit Congestion Notification (ECN) Signaling with Nonces, June 2003. http://tools.ietf.org/html/rfc3540

[21] RFC 4945 The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX, August 2007. http://tools.ietf.org/html/rfc4945

[22] IEEE 802.3 Ethernet Working Group, accessed 9/1/2015. http://www.ieee802.org/3/

[23] Digital Subscriber Line, accessed 9/1/2015. https://en.wikipedia.org/wiki/Digital_subscriber_line

[24] RFC 2516 A Method for Transmitting PPP Over Ethernet (PPPoE), February 1999. http://tools.ietf.org/html/rfc2516

[25] RFC 1122 Requirements for Internet Hosts – Communication Layers, October 1989. http://tools.ietf.org/html/rfc1122

[26] RFC 1123 Requirements for Internet Hosts – Application and Support, October 1989. http://tools.ietf.org/html/rfc1123

[27] Margaret Rouse, OSI reference model (Open Systems Interconnection) definition, accessed 9/1/2015. http://searchnetworking.techtarget.com/definition/OSI

[28] IETF RFC 5246: The Transport Layer Security (TLS) Protocol, Version 1.2, August, 2008. http://tools.ietf.org/html/rfc5246

[29] Netscout Systems, accessed 9/1/2015. https://en.wikipedia.org/wiki/NetScout_Systems

[30] William R. Simpson and Coimbatore Chandersekaran, International Journal of Computer Technology and Application (IJCTA), "An Agent-Based Web-Services Monitoring System," Vol. 2, No. 9, September 2011, pp. 675–685.

[31] William R. Simpson, Coimbatore Chandersekaran and Ryan Wagner, Lecture Notes in Engineering and Computer Science, Proceedings World Congress on Engineering and Computer Science 2011, Volume I, "High Assurance Challenges for Cloud Computing," pp. 61–66, San Francisco, October 2011.

[32] Coimbatore Chandersekaran and William R. Simpson, Lecture Notes in Engineering and Computer Science, Proceedings World Congress on Engineering 2012, The 2012 International Conference of Information Security and Internet Engineering, Volume I, "Claims-Based Enterprise-Wide Access Control," pp. 524–529, London, July 2012.

[33] Coimbatore Chandersekaran and William R. Simpson, International Journal of Scientific Computing, Vol. 6, No. 2, "A Uniform Claims-Based Access Control for the Enterprise," December 2012, ISSN: 0973-578X, pp. 1–23.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
21-10-16	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Enterprise Considerations for Ports and Protocols	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Kevin E. Foltz, William R. Simpson	BC-5-2283
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	NS D-8011 H 2016-000647

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Frank P. Konieczny USAF HQ USAF SAF/CIO A6	SAF/CIO A6
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: William R. Simpson

14. ABSTRACT

The need to control information flow to a restricted set of accepted protocols arises from the vulnerabilities that may come from any protocol. Reducing the acceptable protocols to a small set of well-tested standard protocols will reduce the attack surface and provide high confidence in selected communications. These protocols are restricted to specific ports or addresses in the receiving web service. HTTPS is familiarly restricted to port 443. In the standard nomenclature, this traffic may be configured as either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). The standard ports are defined by Internet Assigned Numbers Authority (IANA). The IANA is responsible for maintaining the official assignments of port numbers for specific uses. However, many unofficial uses of both well-known and registered port numbers occur in practice. Screening of acceptable ports and protocols has been done, in the past, by network appliances known as firewalls. Communications on the approved list were permitted, others blocked. However, many appliances now have such functionality and the server or service may have a host-based security system that can apply this functionality. This paper covers enterprise considerations for screening of ports and protocols.

15. SUBJECT TERMS

Appliance, Firewall, IT Security, Traffic Inspection.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Frank P. Konieczny
Unclassified	Unclassified	Unclassified	Unlimited	6	19b. TELEPHONE NUMBER (Include Area Code) 703-697-1308